Fig. 1

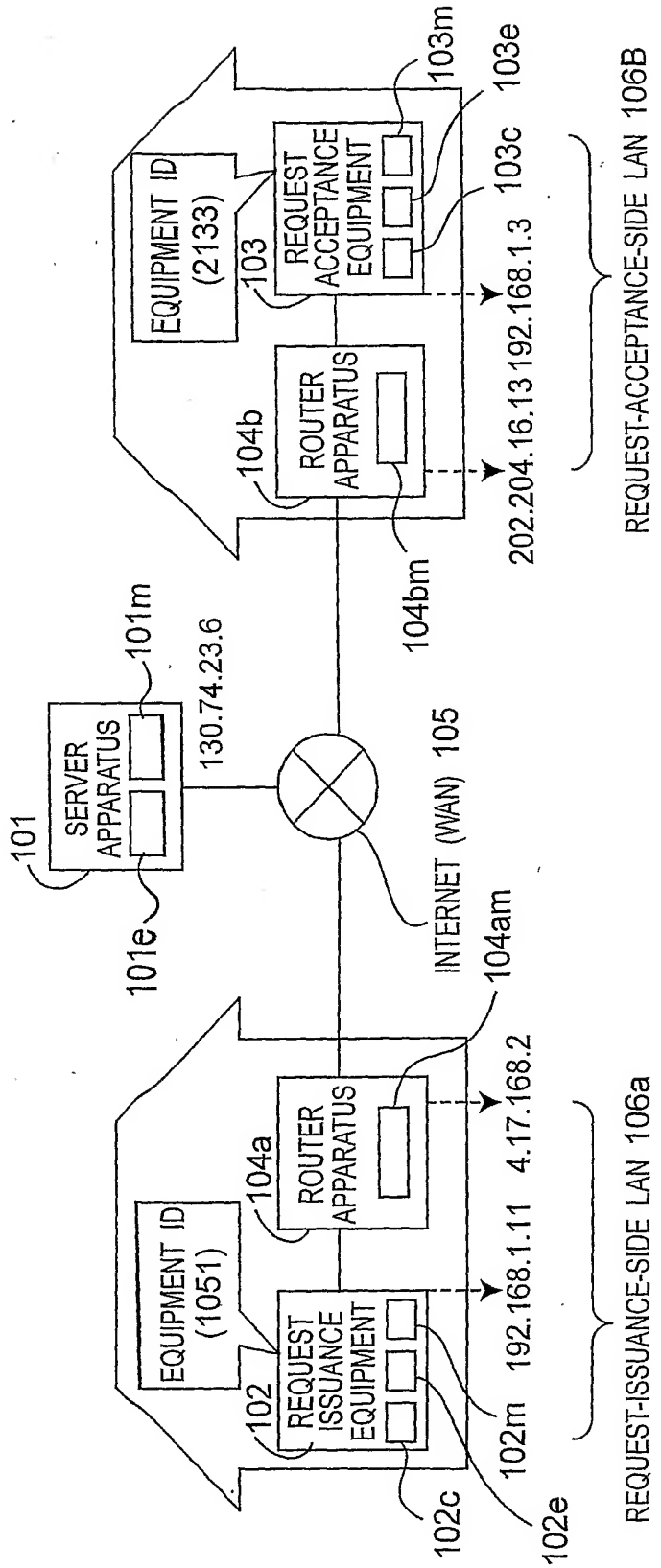

SERVER APPARATUS
101
101e
101m
130.74.23.6
INTERNET (WAN) 105
ROUTER APPARATUS
104a
104am
4.17.168.2
EQUIPMENT ID (1051)
REQUEST ISSUANCE EQUIPMENT
102
102c
102e
102m
192.168.1.11
REQUEST-ISSUANCE-SIDE LAN 106a
ROUTER APPARATUS
104b
104bm
202.204.16.13
192.168.1.3
EQUIPMENT ID (2133)
103
REQUEST ACCEPTANCE EQUIPMENT
103c
103e
103m
REQUEST-ACCEPTANCE-SIDE LAN 106B

Fig.2

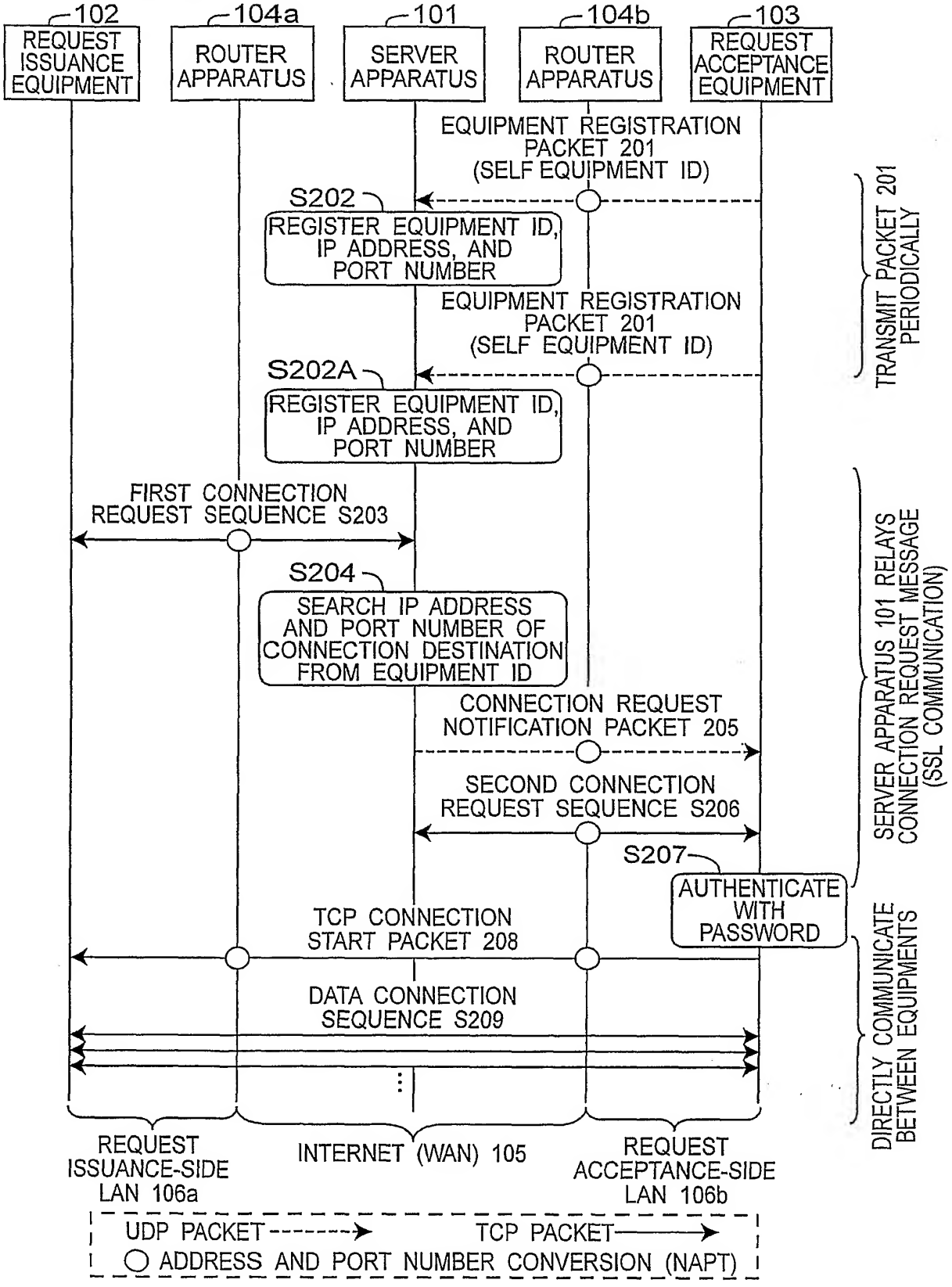

102
REQUEST ISSUANCE EQUIPMENT
104a
ROUTER APPARATUS
101
SERVER APPARATUS
104b
ROUTER APPARATUS
103
REQUEST ACCEPTANCE EQUIPMENT
EQUIPMENT REGISTRATION PACKET 201 (SELF EQUIPMENT ID)
S202
REGISTER EQUIPMENT ID, IP ADDRESS, AND PORT NUMBER
EQUIPMENT REGISTRATION PACKET 201 (SELF EQUIPMENT ID)
TRANSMIT PACKET 201 PERIODICALLY
S202A
REGISTER EQUIPMENT ID, IP ADDRESS, AND PORT NUMBER
FIRST CONNECTION REQUEST SEQUENCE S203
S204
SEARCH IP ADDRESS AND PORT NUMBER OF CONNECTION DESTINATION FROM EQUIPMENT ID
CONNECTION REQUEST NOTIFICATION PACKET 205
SECOND CONNECTION REQUEST SEQUENCE S206
S207
AUTHENTICATE WITH PASSWORD
SERVER APPARATUS 101 RELAYS CONNECTION REQUEST MESSAGE (SSL COMMUNICATION)
TCP CONNECTION START PACKET 208
DATA CONNECTION SEQUENCE S209
DIRECTLY COMMUNICATE BETWEEN EQUIPMENTS
REQUEST ISSUANCE-SIDE LAN 106a
INTERNET (WAN) 105
REQUEST ACCEPTANCE-SIDE LAN 106b
UDP PACKET
TCP PACKET
ADDRESS AND PORT NUMBER CONVERSION (NAPT)

Fig.3

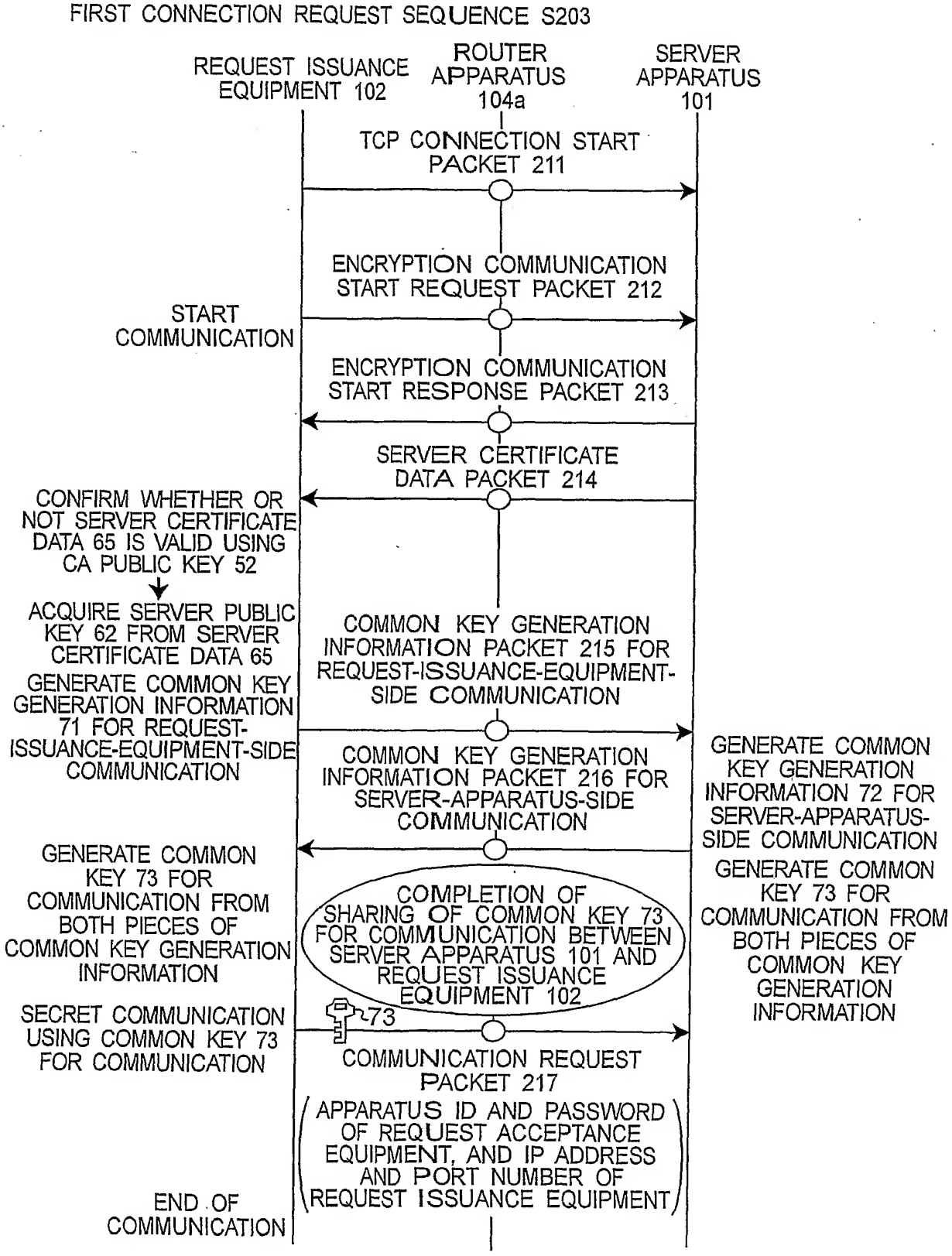

FIRST CONNECTION REQUEST SEQUENCE S203
REQUEST ISSUANCE EQUIPMENT 102
ROUTER APPARATUS 104a
SERVER APPARATUS 101
TCP CONNECTION START PACKET 211
ENCRYPTION COMMUNICATION START REQUEST PACKET 212
START COMMUNICATION
ENCRYPTION COMMUNICATION START RESPONSE PACKET 213
SERVER CERTIFICATE DATA PACKET 214
CONFIRM WHETHER OR NOT SERVER CERTIFICATE DATA 65 IS VALID USING CA PUBLIC KEY 52
ACQUIRE SERVER PUBLIC KEY 62 FROM SERVER CERTIFICATE DATA 65
GENERATE COMMON KEY GENERATION INFORMATION 71 FOR REQUEST-ISSUANCE-EQUIPMENT-SIDE COMMUNICATION
COMMON KEY GENERATION INFORMATION PACKET 215 FOR REQUEST-ISSUANCE-EQUIPMENT-SIDE COMMUNICATION
COMMON KEY GENERATION INFORMATION PACKET 216 FOR SERVER-APPARATUS-SIDE COMMUNICATION
GENERATE COMMON KEY GENERATION INFORMATION 72 FOR SERVER-APPARATUS-SIDE COMMUNICATION
GENERATE COMMON KEY 73 FOR COMMUNICATION FROM BOTH PIECES OF COMMON KEY GENERATION INFORMATION
COMPLETION OF SHARING OF COMMON KEY 73 FOR COMMUNICATION BETWEEN SERVER APPARATUS 101 AND REQUEST ISSUANCE EQUIPMENT 102
GENERATE COMMON KEY 73 FOR COMMUNICATION FROM BOTH PIECES OF COMMON KEY GENERATION INFORMATION
SECRET COMMUNICATION USING COMMON KEY 73 FOR COMMUNICATION
73
COMMUNICATION REQUEST PACKET 217
APPARATUS ID AND PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT, AND IP ADDRESS AND PORT NUMBER OF REQUEST ISSUANCE EQUIPMENT
END OF COMMUNICATION

Fig.4

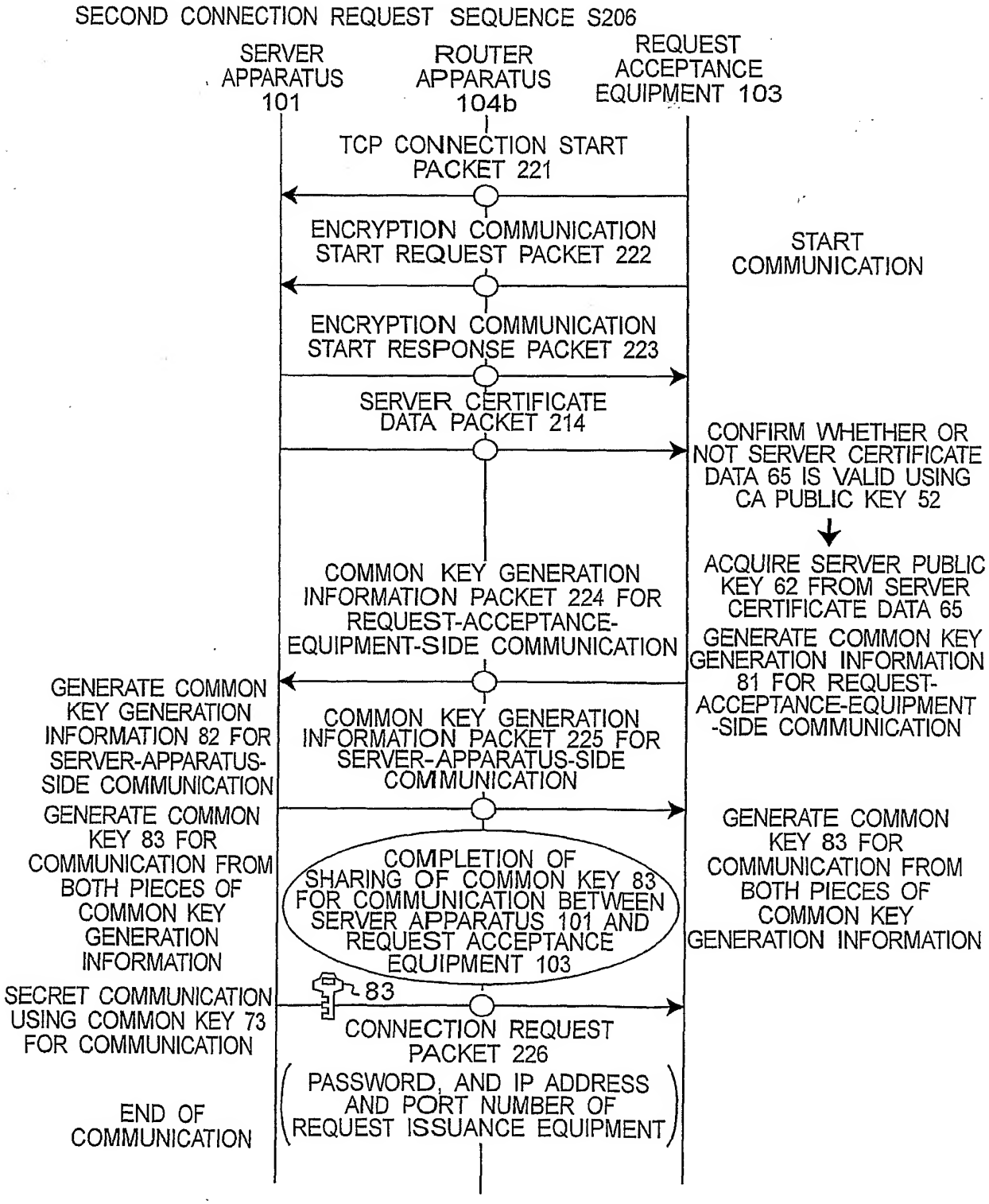

SECOND CONNECTION REQUEST SEQUENCE S206
SERVER APPARATUS 101
ROUTER APPARATUS 104b
REQUEST ACCEPTANCE EQUIPMENT 103
TCP CONNECTION START PACKET 221
ENCRYPTION COMMUNICATION START REQUEST PACKET 222
START COMMUNICATION
ENCRYPTION COMMUNICATION START RESPONSE PACKET 223
SERVER CERTIFICATE DATA PACKET 214
CONFIRM WHETHER OR NOT SERVER CERTIFICATE DATA 65 IS VALID USING CA PUBLIC KEY 52
ACQUIRE SERVER PUBLIC KEY 62 FROM SERVER CERTIFICATE DATA 65
COMMON KEY GENERATION INFORMATION PACKET 224 FOR REQUEST-ACCEPTANCE-EQUIPMENT-SIDE COMMUNICATION
GENERATE COMMON KEY GENERATION INFORMATION 81 FOR REQUEST-ACCEPTANCE-EQUIPMENT -SIDE COMMUNICATION
GENERATE COMMON KEY GENERATION INFORMATION 82 FOR SERVER-APPARATUS-SIDE COMMUNICATION
COMMON KEY GENERATION INFORMATION PACKET 225 FOR SERVER-APPARATUS-SIDE COMMUNICATION
GENERATE COMMON KEY 83 FOR COMMUNICATION FROM BOTH PIECES OF COMMON KEY GENERATION INFORMATION
GENERATE COMMON KEY 83 FOR COMMUNICATION FROM BOTH PIECES OF COMMON KEY GENERATION INFORMATION
COMPLETION OF SHARING OF COMMON KEY 83 FOR COMMUNICATION BETWEEN SERVER APPARATUS 101 AND REQUEST ACCEPTANCE EQUIPMENT 103
83
SECRET COMMUNICATION USING COMMON KEY 73 FOR COMMUNICATION
CONNECTION REQUEST PACKET 226
(PASSWORD, AND IP ADDRESS AND PORT NUMBER OF REQUEST ISSUANCE EQUIPMENT)
END OF COMMUNICATION

Fig.5

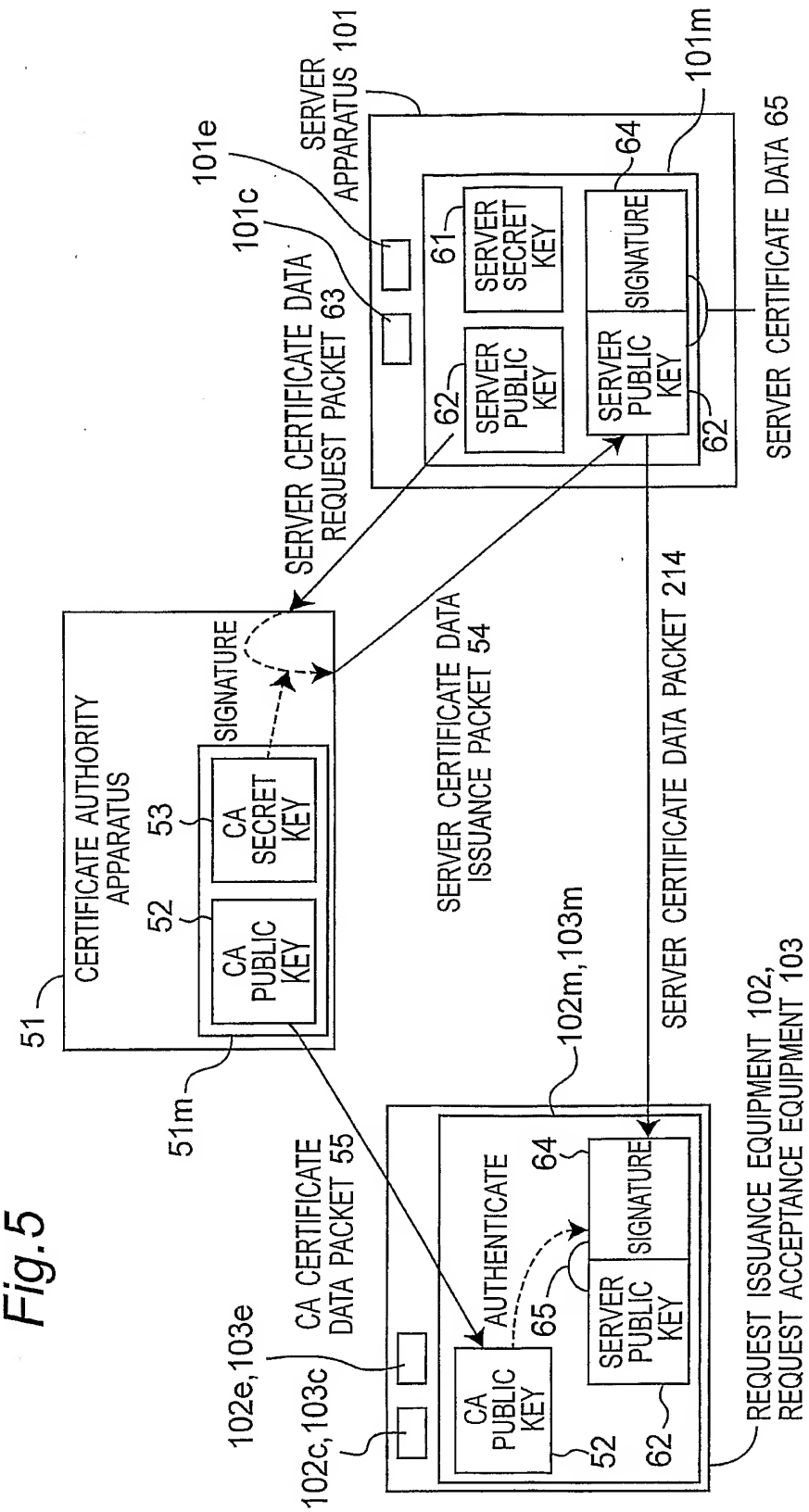

SERVER APPARATUS 101
101e
101c
101m
SERVER CERTIFICATE DATA REQUEST PACKET 63
SERVER SECRET KEY
SERVER PUBLIC KEY
SIGNATURE
SERVER CERTIFICATE DATA 65
CERTIFICATE AUTHORITY APPARATUS
CA PUBLIC KEY
CA SECRET KEY
SIGNATURE
SERVER CERTIFICATE DATA ISSUANCE PACKET 54
SERVER CERTIFICATE DATA PACKET 214
51
51m
102m,103m
CA CERTIFICATE DATA PACKET 55
AUTHENTICATE
102e,103e
102c,103c
REQUEST ISSUANCE EQUIPMENT 102, REQUEST ACCEPTANCE EQUIPMENT 103

Fig.6

104am

LAN EQUIPMENT ADDRESS	WAN ROUTER ADDRESS	LAN EQUIPMENT PORT NUMBER	WAN ROUTER PORT NUMBER
192.168.1.11	4.17.168.2	1500	7000
192.168.1.11	4.17.168.2	1600	5000
---	---	---	---

← FOR TCP COMMUNICATION WITH SERVER APPARATUS 101

← FOR TCP COMMUNICATION WITH REQUEST ACCEPTANCE EQUIPMENT 103

Fig.7A

EQUIPMENT REGISTRATION PACKET 201 (LAN SIDE)

SA= 192.168.1.3
DA= 130.74.23.6
SP= 2000
DP= 1200
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.7B

EQUIPMENT REGISTRATION PACKET 201 (WAN SIDE)

SA= 202.204.16.13
DA= 130.74.23.6
SP= 3400
DP= 1200
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.7C

CONNECTION REQUEST PACKET 217 (LAN SIDE)

SA= 192.168.1.11
DA= 130.74.23.6
SP= 1500
DP= 1201
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST-ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST-ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.7D

CONNECTION REQUEST PACKET 217 (WAN SIDE)

SA= 4.17.168.2
DA= 130.74.23.6
SP= 7000
DP= 1201
EQUIPMENT ID OF REQUEST ACCEPTANCE EQUIPMENT 103 (2133)
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST-ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST-ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.8A

CONNECTION REQUEST NOTIFICATION PACKET 205 (LAN SIDE)

SA= 130.74.23.6
DA= 192.168.1.3
SP= 1200
DP= 2000
CONNECTION REQUEST NOTIFICATION FLAG

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.8B

CONNECTION REQUEST NOTIFICATION PACKET 205 (WAN SIDE)

SA= 130.74.23.6
DA= 202.204.16.13
SP= 1200
DP= 2400
CONNECTION REQUEST NOTIFICATION FLAG

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.8C

CONNECTION REQUEST PACKET 226 (LAN SIDE)

SA= 130.74.23.6
DA= 192.168.1.3
SP= 1300
DP= 2600
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST-ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST-ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.8D

CONNECTION REQUEST PACKET 226 (WAN SIDE)

SA= 130.74.23.6
DA= 202.204.16.13
SP= 1300
DP= 2401
PASSWORD OF REQUEST ACCEPTANCE EQUIPMENT 103
IP ADDRESS OF REQUEST-ISSUANCE-SIDE LAN 106a (4.17.168.2)
PORT NUMBER OF REQUEST-ISSUANCE-SIDE LAN 106a (5000)

SA: SOURCE ADDRESS FIELD
DA: DESTINATION ADDRESS FIELD
SP: SOURCE PORT NUMBER FIELD
DP: DESTINATION PORT NUMBER FIELD

Fig.9

101m

EQUIPMENT ID	IP ADDRESS	PORT NUMBER
2133	202.204.16.13	3400
---	---	---
---	---	---

Fig.10

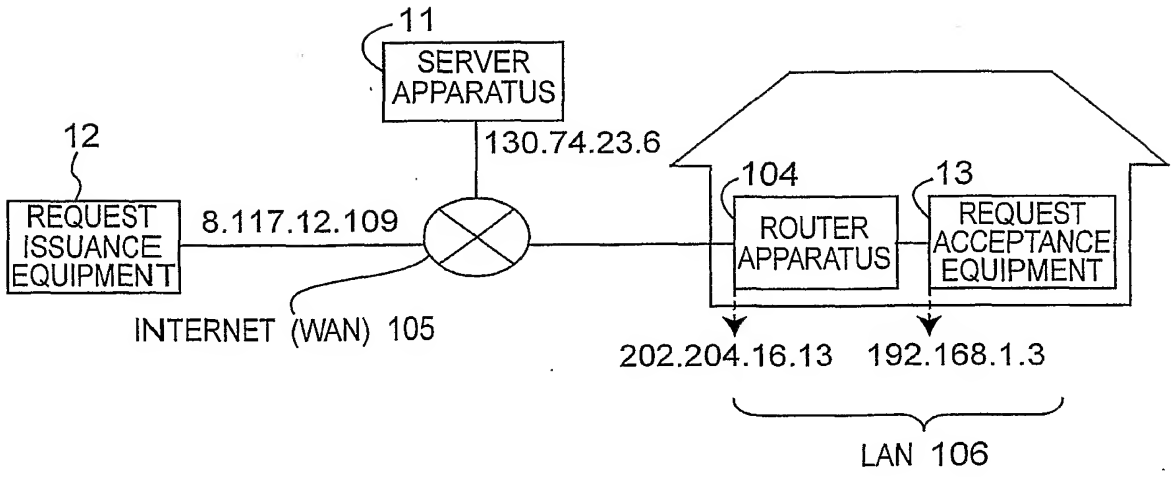


Fig.11

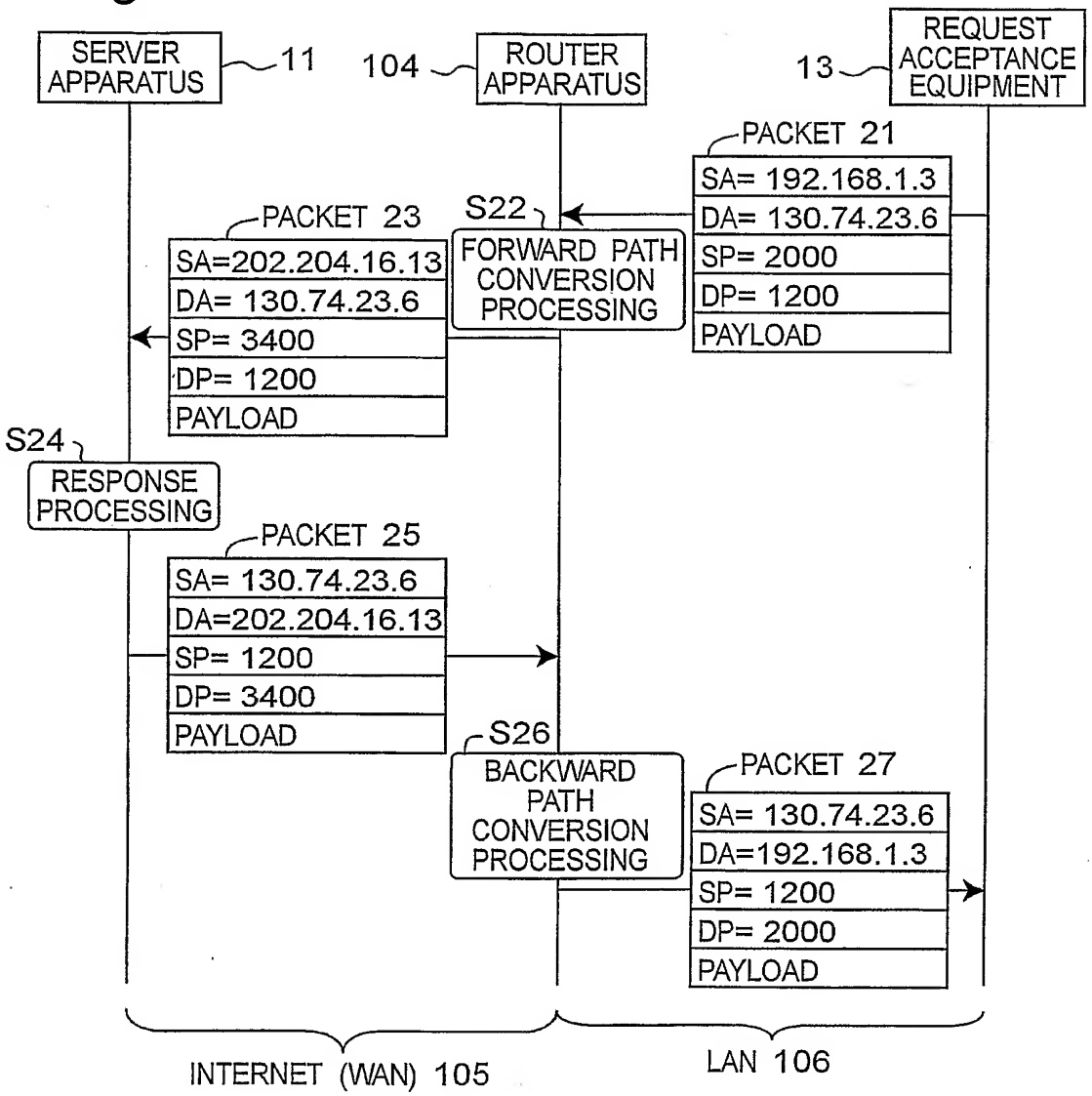
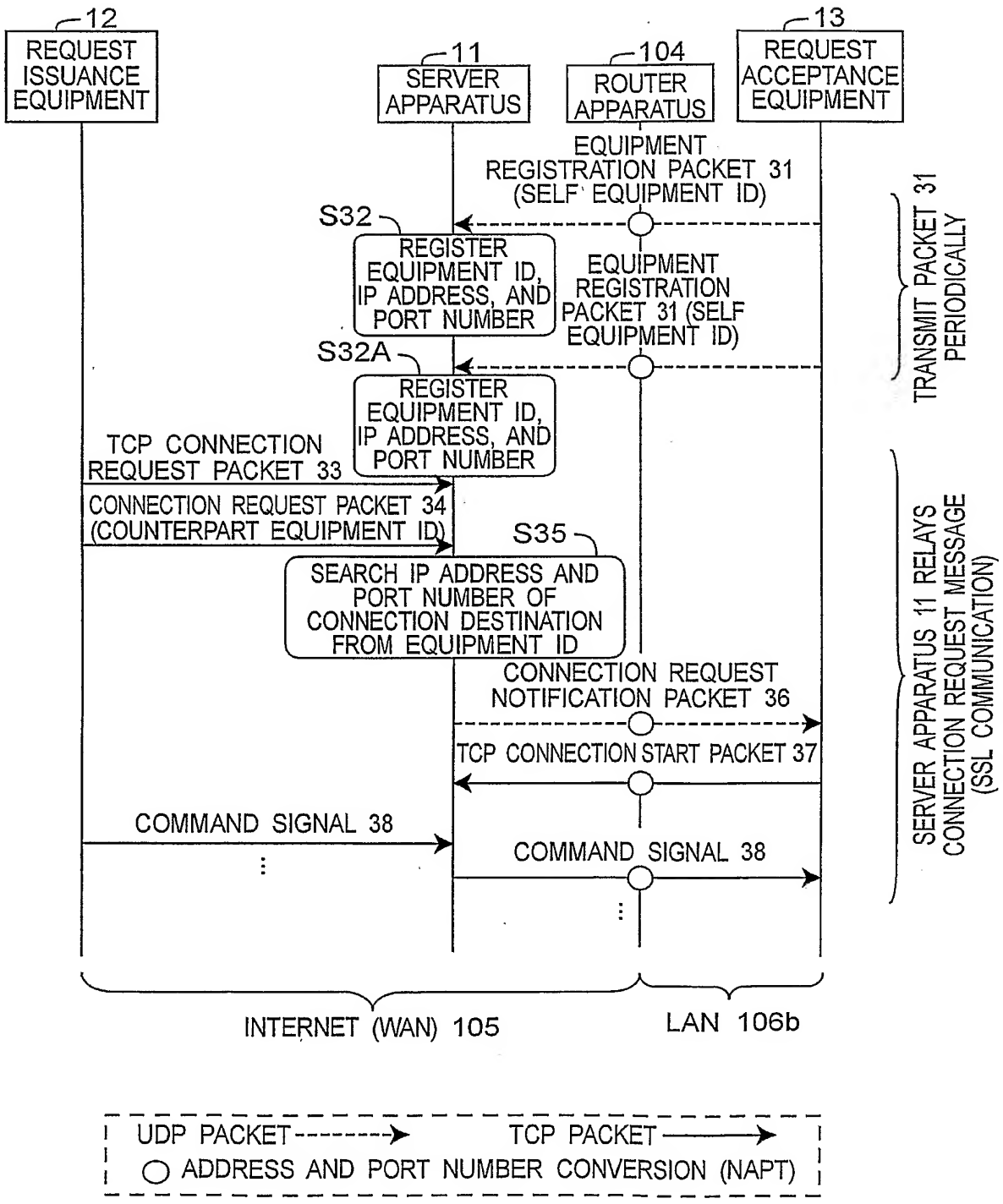


Fig.12

LAN EQUIPMENT ADDRESS	WAN ROUTER ADDRESS	LAN EQUIPMENT PORT NUMBER	WAN ROUTER PORT NUMBER
192.168.1.3	202.204.16.13	2000	3400
---	---	---	---
---	---	---	---

Fig.13


12
REQUEST ISSUANCE EQUIPMENT
11
SERVER APPARATUS
104
ROUTER APPARATUS
13
REQUEST ACCEPTANCE EQUIPMENT
EQUIPMENT REGISTRATION PACKET 31 (SELF EQUIPMENT ID)
S32
REGISTER EQUIPMENT ID, IP ADDRESS, AND PORT NUMBER
EQUIPMENT REGISTRATION PACKET 31 (SELF EQUIPMENT ID)
S32A
REGISTER EQUIPMENT ID, IP ADDRESS, AND PORT NUMBER
TRANSMIT PACKET 31 PERIODICALLY
TCP CONNECTION REQUEST PACKET 33
CONNECTION REQUEST PACKET 34 (COUNTERPART EQUIPMENT ID)
S35
SEARCH IP ADDRESS AND PORT NUMBER OF CONNECTION DESTINATION FROM EQUIPMENT ID
CONNECTION REQUEST NOTIFICATION PACKET 36
TCP CONNECTION START PACKET 37
COMMAND SIGNAL 38
COMMAND SIGNAL 38
SERVER APPARATUS 11 RELAYS CONNECTION REQUEST MESSAGE (SSL COMMUNICATION)
INTERNET (WAN) 105
LAN 106b
UDP PACKET
TCP PACKET
ADDRESS AND PORT NUMBER CONVERSION (NAPT)